



Zugriff auf ONTAP tools für VMware vSphere Wartungskonsole

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

Inhalt

- Zugriff auf ONTAP tools für VMware vSphere Wartungskonsole 1
 - Erfahren Sie mehr über die ONTAP tools maintenance console 1
 - Konfigurieren Sie den Ferndiagnosezugriff für ONTAP tools 2
 - Starten Sie SSH auf anderen ONTAP tools-Knoten. 3
 - Aktualisieren Sie die vCenter Server-Anmeldeinformationen in ONTAP tools. 3
 - Ändern Sie das Zertifikatvalidierungsflag in ONTAP tools 3
 - SAN-basierte Zertifikate für Storage-Backends überprüfen. 4

Zugriff auf ONTAP tools für VMware vSphere Wartungskonsole

Erfahren Sie mehr über die ONTAP tools maintenance console

Die Wartungskonsole für ONTAP tools for VMware vSphere ermöglicht die Verwaltung von Anwendungs-, System- und Netzwerkeinstellungen. Administrator- und Wartungskennwörter lassen sich aktualisieren, Support-Bundles generieren, Protokollierungsstufen konfigurieren, TLS-Einstellungen verwalten und die Remote-Diagnose aktivieren.

Nach der Bereitstellung von ONTAP tools for VMware vSphere ist bei nicht erreichbarer Wartungskonsole die Installation der VMware tools vom vCenter Server erforderlich. Die Anmeldung erfolgt mit dem `maint` Benutzernamen und dem während der Bereitstellung festgelegten Passwort. **nano** steht zum Bearbeiten von Dateien in der Wartungs- oder Root-Anmeldekonsole zur Verfügung.



Für den `diag`-Benutzer sollte beim Aktivieren der Diagnose ein Passwort festgelegt werden.

Die Registerkarte **Zusammenfassung** der bereitgestellten ONTAP tools for VMware vSphere bietet Zugriff auf die Wartungskonsole. Bei Auswahl von  startet die Wartungskonsole.

Konsolenmenü	Optionen
Anwendungskonfiguration	1. Serverstatusübersicht 2. Protokollebene für ONTAP tools Dienste ändern 3. Zertifikatvalidierungs-Flag ändern
Systemkonfiguration	1. Virtuelle Maschine neu starten 2. Virtuelle Maschine herunterfahren 3. 'maint'-Benutzerpasswort ändern 4. Zeitzone ändern 5. Jail-Datenträgergröße (/jail) erhöhen 6. Upgrade 7. VMware Tools installieren

Netzwerkconfiguration	1. IP-Adresseinstellungen anzeigen 2. Einstellungen für die Domainnamensuche anzeigen 3. Einstellungen für die Domainnamensuche ändern 4. Statische Routen anzeigen 5. Statische Routen ändern 6. Änderungen übernehmen 7. Einen Host anpingen 8. Standardeinstellungen wiederherstellen
Support und Diagnose	1. Zugriff auf die Diagnose-Shell 2. Remote-Diagnosezugriff aktivieren 3. Anmeldedaten für vCenter zur Sicherung bereitstellen 4. Backup erstellen

Konfigurieren Sie den Ferndiagnosezugriff für ONTAP tools

Sie können ONTAP tools for VMware vSphere so konfigurieren, dass der SSH-Zugriff für den diag-Benutzer aktiviert wird.

Bevor Sie beginnen

Die VASA Provider Erweiterung für Ihre vCenter Serverinstanz aktivieren.

Über diese Aufgabe

Die Verwendung von SSH für den Zugriff auf das diag-Benutzerkonto hat folgende Einschränkungen:

- Pro SSH-Aktivierung ist nur ein Login-Konto zulässig.
- Der SSH-Zugriff auf das diag-Benutzerkonto ist deaktiviert, wenn eine der folgenden Bedingungen eintritt:
 - Die Zeit ist abgelaufen.

Die Anmeldesitzung läuft am nächsten Tag um Mitternacht ab.

- Sie melden sich erneut als diag-Benutzer per SSH an.

Schritte

1. Vom vCenter Server aus eine Konsole zum VASA Provider öffnen.
2. Melden Sie sich als Wartungsb Benutzer an.
3. Geben Sie 4 ein, um **Support und Diagnose** auszuwählen.
4. Drücken Sie 2, um **Remote-Diagnosezugriff aktivieren** auszuwählen.
5. Geben Sie y im Bestätigungsdiaologfeld ein, um den Remote-Diagnosezugriff zu aktivieren.
6. Ein Passwort für den Ferndiagnosezugriff eingeben.

Starten Sie SSH auf anderen ONTAP tools-Knoten

SSH muss auf anderen Knoten gestartet werden, bevor das Upgrade erfolgt.

Bevor Sie beginnen

Die VASA Provider Erweiterung für Ihre vCenter Serverinstanz aktivieren.

Über diese Aufgabe

Dieser Vorgang ist auf jedem Knoten vor dem Upgrade zu wiederholen.

Schritte

1. Vom vCenter Server aus eine Konsole zum VASA Provider öffnen.
2. Melden Sie sich als Wartungsbenutzer an.
3. Geben Sie 4 ein, um Support und Diagnose auszuwählen.
4. Drücken Sie die Eingabetaste 1, um die Access Diagnostic Shell auszuwählen.
5. Geben Sie y ein, um fortzufahren.
6. Der Befehl `sudo systemctl restart ssh` wird ausgeführt.

Aktualisieren Sie die vCenter Server-Anmeldeinformationen in ONTAP tools

Sie können die Anmeldeinformationen der vCenter Serverinstanz über die Wartungskonsole aktualisieren.

Bevor Sie beginnen

Sie benötigen die Anmeldedaten für den Wartungsbenutzer.

Über diese Aufgabe

Wenn die vCenter Server-Zugangsdaten nach der Bereitstellung geändert wurden, können sie mit diesem Verfahren aktualisiert werden.

Schritte

1. Vom vCenter Server aus eine Konsole zum VASA Provider öffnen.
2. Melden Sie sich als Wartungsbenutzer an.
3. Geben Sie 2 ein, um das Menü Systemkonfiguration auszuwählen.
4. Geben Sie 8 ein, um die vCenter-Anmeldedaten zu ändern.

Ändern Sie das Zertifikatvalidierungsflag in ONTAP tools

Standardmäßig ist die Zertifikatsvalidierungs-Flag aktiviert (auf true gesetzt). Das ONTAP Speicher-Backend Zertifikatsvalidierungs-Flag kann auf false gesetzt werden, wenn eine Umgehung der SAN-Zertifikatsprüfung erforderlich ist. Diese Einstellung ist nicht anwendbar auf vCenter Server-Zertifikate.

Bevor Sie beginnen

Sie benötigen die Anmeldedaten für den Wartungsbenutzer.

Schritte

1. Vom vCenter Server aus eine Konsole zu ONTAP tools öffnen.
2. Melden Sie sich als Wartungsbenutzer an.
3. Geben Sie 1 ein, um das Menü **Application Configuration** auszuwählen.
4. Geben Sie 3 ein, um das Zertifikatvalidierungsflag zu ändern.

Die Wartungskonsole zeigt den Status des Zertifikatvalidierungsflags an und fordert Sie auf, ihn zu ändern.

5. Geben Sie 'y' ein, um das Flag umzuschalten, oder 'n', um abubrechen.

Wenn die Zertifikatsvalidierungs-Flagge aktiviert ist (auf „true“ gesetzt), prüft ONTAP tools, ob alle Storage-Backends Zertifikate mit einem Subject Alternative Name (SAN) verwenden. Wenn ein Backend ein Zertifikat ohne SAN verwendet, kann die Zertifikatsvalidierung nicht aktiviert werden. Vor der Aktivierung dieser Flagge sollte überprüft werden, dass alle Storage-Backends SAN-basierte Zertifikate verwenden. Wenn die Zertifikatsvalidierungs-Flagge deaktiviert ist (auf „false“ gesetzt), überspringen ONTAP tools die Zertifikatsvalidierung für alle konfigurierten Storage-Backends.

SAN-basierte Zertifikate für Storage-Backends überprüfen

Um eine sichere Kommunikation und ordnungsgemäße Validierung zu gewährleisten, überprüfen Sie, ob alle Storage-Backends SAN-basierte Zertifikate verwenden:

1. Prüfen Sie, ob das ONTAP-Managementzertifikat einen Subject Alternative Name (SAN)-Eintrag enthält.
2. Bestätigen Sie, dass die SAN-Einträge mit der ONTAP-Management-IP-Adresse oder dem DNS-Namen oder beiden übereinstimmen.
3. Stellen Sie sicher, dass die für die Onboarding von ONTAP verwendeten Details mit der IP-Adresse oder dem DNS-Namen im SAN-Eintrag des Zertifikats übereinstimmen.

Durch die Befolgung dieser Schritte lassen sich Probleme bei der Zertifikatsvalidierung vermeiden und sicherstellen, dass das ONTAP-System sicher integriert ist.

Das folgende Beispielzertifikat zeigt die dekodierten Informationen:

```
HG8u6GK r2JJonWe/kjoKTUnkjwtW7feDI747RUuFrthcvTDqhBNWL76jihNp1VX7
v0SDWMAVdecTeU1X/1X3qMxiL+tU4p9SbKVpQw6hjm/zi0LNC784EYIOSQ7qVob
6f21mfPOJHbqs5fLim9NFFUu2DQIDAQA8oQw0jBABgNVHREEOT43hwShsSHdKXsgi9z
dGkyMjAtdnNpbS1zcjA1MWUtY2OuY2Rs LmdkbC5lbmdsYWJuZKThcPHauY29nt
BgkqhkiG9wQBAQsFAAOCCAQAEEagptz11RN7PLuJUo-SSQExBsF5/3JHr0+sSIMZDzm
4P24kbxQZbfryy68itKGF4LeAid0hgyxc3y9iv4zKlx8SfLNgiTnVqAe8'KYNoyD6
IEwppDUE0eVNIZQjrz9QjUAAF9ifjq8+SKr'lphoXnYYUiM6utvobPMG8cR8Gca
jiLibiMM01K6rD7Ng+7+ydUCAwBQwMDDwdn8+7RIRdKgwx9QDLegcC5IL5WFLwbMc
2GBv8VM839m0KUAKXSDGwJBZ5nSHQdNi7MU3AES7Nzkv63kGEQJT/5Wr1DmOwlf
osl4qeeeMRigrAbFL6EHMsOMSP0521rtTrJrjBooB22r0tyDA--
-----END CERTIFICATE-----
```

Certificate Information:

- ✓ Common Name: **test.xyz.com**
- ✓ Subject Alternative Names: IP Address: **xxx.xx.xxx.xxx**, **test.xyz.com**
- ✓ Organization: Self-signed-certificate
- ✓ Organization Unit:
- ✓ Locality: N/A
- ✓ State: N/A
- ✓ Country: XX
- ✓ Valid From: March 8, 2026
- ✓ Valid To: March 7, 2028
- ✓ Issuer: **test.xyz.com**, Self-signed-certificate
- ✓ Serial Number: 640c2752bd2c972c5775180070cfdd2120809ee

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.